UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,046	07/12/2001	Christine Cheng	3801.P042	3861

21186 7590 06/01/2006

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
OYEBISI, OJO O	

ART UNIT	PAPER NUMBER
3628	

DATE MAILED: 06/01/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/905,046	CHENG ET AL.	
	Examiner	Art Unit	
	OJO O. OYEBISI	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *7/12/01* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/12/01, 7/12/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 33-40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 33 through 40 are system claims, but appear to be directed to software per se. That is to say, claims 33-40 only recite software without any structure limitations to be a system.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-6, 31-36, and 40 are rejected under 35 U.S.C. 102(b) as being anticipated by Trostle (US PAT: 5,919,257).

Re claims 1 and 2. Trostle teaches a method to detect fraudulent activities at a network-based transaction facility, the method comprising: causing a first identifier (i.e., authorized username) associated with a first user identity to be stored on a machine responsive to a first event with respect to the network-based transaction facility and initiated under the first user identity from the machine which is coupled to the network-based transaction facility via a network; and detecting a potentially fraudulent activity

by detecting a lack of correspondence (i.e., In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends, see col.5 lines 45-55) between the first identifier stored on the machine and a second identifier (i.e., entered username) associated with a second user identity responsive to a second event with respect to the network-based transaction facility and initiated under the second user identity from the machine (i.e., In step 82 a username prompt is presented to the user. In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88. The encrypted private key can only be decrypted with the user's password. In step 90 the server checks if any login restrictions, such as, time restrictions, station restrictions and account lock-out restrictions have been violated. These restrictions prevent logins from unauthorized workstations or logins during the wrong time of day. If there are violations, access is denied (step 86). However, if there are no login restrictions, the user is prompted to enter a password in step 92 and the validity of the password is determined in step 94, see col.5 lines 45-67).

Re claims 31-33, and 40. Claims 31-33, and 40 recite similar limitations to claim 1 and thus rejected using the same art and rationale in the rejection of claim 1.

Re claims 3 and 34. Trostle discloses a method comprising causing the lack of correspondence between the first identifier and second identifier to be detected at the machine (i.e., In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends, see col.5 lines 45-55).

Re claims 4-6, 35-36. Trostle further discloses a method comprising receiving both the first identifier and the second identifier at the network-based transaction facility from the machine, and detecting the lack of correspondence between the first identifier and second identifier at the network-based transaction facility (i.e., In step 82 a username prompt is presented to the user. In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88, see col.5 lines 45-60).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 7-8, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle.

Re claims 7-8, and 37. Trostle does not explicitly disclose a method comprising causing the first and second identifier to be stored on the machine within a cookie. However, storing user identifiers on the machine within a cookie is a well-known cookie bundling scheme. Cookie bundling is a common practice wherein all of the separate cookies pertaining to different type of user transaction preferences are packed together into one file. Thus it would have been obvious to one of ordinary skill in the art to introduce the well-known scheme in Trostle to enable separate cookies pertaining to different type of user transaction preferences to be packed together into one file.

7. Claims 9-19, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Miller (Michael Miller, The complete Idiot's Guide to Ebay Online Auctions, copyright July 1999).

Re claims 9, 10. Trostle does not explicitly disclose a method wherein the first event includes one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility. However, Miller discloses a method wherein the first event includes one of registering with the network-based transaction facility (see pg 133), communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based

transaction facility (i.e., ebay, see pg 52) communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility (i.e., ebay feedback, see pgs 157-161). Thus it would have been obvious to incorporate what is taught by Miller into Trostle to allow individuals and small businesses to sell and buy items from other internet users worldwide.

Re claims 11-14, and 38. Trostle discloses the method comprising: the detection of the lack of correspondence between the first identifier and the second identifier at one of the machine and the network-based transaction facility; inspect for the potentially fraudulent activity (i.e., In step 82 a username prompt is presented to the user. In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88, see col.5 lines 45-60), and causing the potentially fraudulent activity to be recorded into a database. (i.e., If the values are equal then illicit changes have not been made to the selected executables programs, and execution continues with step 90 which returns workstation execution to the system BIOS. Otherwise, step 92 is performed to notify the user, and/or the network system administrator, that an unauthorized change has been detected. The workstation may also make an entry in an **audit server audit log,** see col.7 lines 27-38). Trostle does not explicitly disclose causing the first identifier and the second identifier to be stored on the machine within a shill cookie; causing a cookie identifier to be stored within the shill

cookie; causing the shill cookie to be coupled to a cookie bundle which records a plurality of transaction preferences for the first user identity and the second user identity on the machine; causing the shill cookie bundle to be sent from the machine to the network-based transaction facility when the second user identify makes the second transaction event with the network-based transaction facility using the machine; causing the shill cookie to be appended with the second identifier. However, storing user identifiers on the machine within a cookie is a well-known cookie bundling scheme. Cookie bundling is a common practice wherein all of the separate cookies pertaining to different type of user transaction preferences are packed together into one file. Thus it would have been obvious to one of ordinary skill in the art to introduce the well-known scheme in Trostle/Miller to enable separate cookies pertaining to different type of user transaction preferences to be packed together into one file.

Re claim 15. Trostle discloses a method wherein the machine comprises a computer connected to the network-based transaction facility (i.e., a networked workstation performs an intrusion detection hashing function on selected workstation executable programs, see abstract).

Re claim 16. Trostle does not explicitly disclose a method wherein the network-based transaction facility comprises an Internet-based auction facility. However Miller makes this disclosure (i.e., ebay, see pg 52). Thus it would have been obvious to incorporate what is taught by Miller into Trostle to allow individuals and small businesses to sell items to sell and buy items from other internet users worldwide.

Re claim 17. Trostle does not explicitly disclose a method as in claim 16 further comprising: causing the shill cookie to record and to store a predetermined number of user identifiers. However, storing/recording user identifiers on the machine within a cookie is a well-known cookie bundling scheme. Cookie bundling is a common practice wherein all of the separate cookies pertaining to different type of user transaction preferences are packed together into one file. Thus it would have been obvious to one of ordinary skill in the art to introduce the well-known scheme in Trostle/Miller to enable separate cookies pertaining to different type of user transaction preferences to be packed together into one file.

Re claims 18 and 19. Trostle does not disclose a method further comprising causing the shill cookie and the cookie bundle to be encoded and encrypted such that the shill cookie and the bundle cookie are coded. However, encoding and encrypting cookie are old and well known in the art. Encoding a cookie is formatting a cookie into a language that is not readily apparent to the user. Thus it would have been obvious to one of ordinary skill in the art to incorporate what is old and well known in the art into Trostle/Miller to maintain data integrity and to guarantee transaction facility security.

8. Claims 20-30, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Miller as applied to claims 19 and 38 above and further in view of Smaha et al (Smaha hereinafter, US PAT: 5,557,742).

Re claims 20-21, and 39. Neither Trostle nor Miller explicitly disclose a method further comprising: generating a potential fraudulent activities table having a fraudulent activity

field, a cookie identifier field, a user identifier field, and a frequency field; recording each of the potentially fraudulent activities and corresponding information into the potential fraudulent activities table; updating the potential fraudulent activities table at least on a periodic basis; and providing an updated report of the potential fraudulent activities table to an investigation team. However, Smaha discloses generating a potential fraudulent activities table having a fraudulent activity field, a cookie identifier field, a user identifier field, and a frequency field (i.e., generate misuse report and load pres-elected fields, see fig.6B element 170 and element 176); recording each of the potentially fraudulent activities (i.e., misuse) and corresponding information into the potential fraudulent activities table (see fig.4 element 126); updating the potential fraudulent activities table at least on a periodic basis (i.e., once a misuse has been detected, an output mechanism generates a signal for use by notification and storage mechanism, see col.3 lines 40-45, also see col.6 lines 11-14); and providing an updated report of the potential fraudulent activities table to an investigation team (i.e., the detection system then generates a text-based output report for a user to view or stored, see col.3 lines 40-44). Thus it would have been obvious to one of ordinary skill in the art to combine Trostle, Miller and Smaha to enable a user to store, view and analyze the fraudulent activities.

Re claim 22. Trostle does not explicitly disclose a method wherein the new event includes one of registering with the network-based transaction facility, communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility, communicating a feedback regarding a transaction, and updating a profile maintained

by the network-based transaction facility. However, Miller discloses a method wherein the new event includes one of registering with the network-based transaction facility (see pg 133), communicating an offer to sell an offering via the network-based transaction facility, communicating and offering to purchase the offering via the network-based transaction facility (i.e., ebay, see pg 52) communicating a feedback regarding a transaction, and updating a profile maintained by the network-based transaction facility (i.e., ebay feedback, see pgs 157-161). Thus it would have been obvious to incorporate what is taught by Miller into Trostle to allow individuals and small businesses to sell and buy items from other internet users worldwide.

Re claims 23 and 24. Neither Trostle nor Miller discloses a method comprising providing the updated report to the investigation team at a predetermined time. However, Shama discloses providing the updated report to the investigation team (i.e., a user) at a predetermined time (i.e., the detection system then generates a text-based output report for a user to view or stored, see col.3 lines 40-44). Thus it would have been obvious to one of ordinary skill in the art to combine Trostle, Miller and Smaha to enable a user to store, view and analyze the fraudulent activities.

Re claim 25. Neither Trostle nor Miller and Shama a method further comprising providing a priority ranking system having a low priority for a low potential fraudulent activity frequency, a medium priority for a medium potential fraudulent activity frequency and a high priority for a high potential fraudulent activity frequency. However, it is old and well in business management art to prioritize events based on the events degree of importance. Thus it would have been obvious to one of ordinary skill in the art to

incorporate what is old and well known in the art into the combination of Trostle, Miller and Shama to prioritize the frequency of fraudulent activities and to enable the system to process data more efficiently.

Re claim 26. Trostle discloses a method further comprising examining the updated report to confirm the potentially fraudulent activity (i.e., the detection system then generates a text-based output report for a user to view or stored, see col.3 lines 40-44).

Re claim 27. Trostle discloses how fraudulent activities i.e., an authorized change to a workstation can be detected and prevented. Trostle does not explicitly disclose a method wherein the potentially fraudulent activity includes one of shill biddings and shill feedbacks. However, Miller explicitly disclose a method wherein the potentially fraudulent activity includes one of shill biddings and shill feedbacks (see pg 218 and pg 222). Thus it would have been obvious to one of ordinary skill in the art to use the intrusion detection system of Trostle to detect and prevent fraudulent activities in online auction market i.e., shill bidding and shill feedback as taught by Miller.

Re claim 28. Trostle does not disclose a method wherein the recording does not affect any one of the first event, the second event, and the new event. However Smaha makes this disclosure (i.e., a method for using processing system inputs to form events, processing the events by the misuse engine according to a set of selectable misuses, and generating one or more misuse outputs. The method converts system-generated inputs to events by establishing a first data structure for use by the system which stores the event. The data structure has elements including (1) authentication information; (2) subject information; and (3) object information. The method further extracts from

system audit trail records, system log file data, and system security state data the information necessary for the first data structure. The method includes the steps of storing the events into the first data structure, see col.12 line 65 – col.13 line10). Thus it would have been obvious to combine the teachings of Trostle and Smaha to detect and prevent fraudulent activities in online auction market.

Re claim 29. Trostle further discloses a method further comprising causing the detection of the potentially fraudulent activity responsive a matching of at least two user transaction preferences from at least two different user identifies (i.e., In step 82 a username prompt is presented to the user. In response, the user enters a username which is transmitted to the server and in step 84 the server compares the entered username against a list of authorized users. If the username is not valid, network access is denied in step 86 and the login process ends. However, if the entered username is on the list, the server returns an encrypted private key to the workstation in step 88. The encrypted private key can only be decrypted with the user's password. In step 90 the server checks if any login restrictions, such as, time restrictions, station restrictions and account lock-out restrictions have been violated. These restrictions prevent logins from unauthorized workstations or logins during the wrong time of day. If there are violations, access is denied (step 86). However, if there are no login restrictions, the user is prompted to enter a password in step 92 and the validity of the password is determined in step 94, see col.5 lines 45-67).

Re claim 30. Trostle does not explicitly discloses a method wherein the user transaction preferences comprise credit card numbers, bidding histories, payment

methods, and shipping addresses. However, Miller makes this disclosure (see pg 23). Thus it would have been obvious to one of ordinary skill in the art to combine the teachings of Trostle and Miller to detect and prevent fraudulent activities in online auction market.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to OJO O. OYEBISI whose telephone number is (571) 272-8298. The examiner can normally be reached on 8:30A.M-5:30P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, HYUNG S. SOUGH can be reached on (571)272-6799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HYUNG SOUGH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600